



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/709,751	05/26/2004	Fonda J. Daniels	014682.000007	3750

44870 7590 06/04/2007  
MOORE & VAN ALLEN, PLLC For IBM  
P.O. Box 13706  
Research Triangle Park, NC 27709

EXAMINER
----------

SANDERS, AARON J

ART UNIT	PAPER NUMBER
----------	--------------

2168

MAIL DATE	DELIVERY MODE
-----------	---------------

06/04/2007

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/709,751	<b>Applicant(s)</b> DANIELS ET AL.	
	<b>Examiner</b> Aaron Sanders	<b>Art Unit</b> 2168	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 24 April 2007.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1,4-7,9,11-16,18,20-24,27,28,30,32,33,35,36,38,40,41 and 43-45 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,4-7,9,11-16,18,20-24,27,28,30,32,33,35,36,38,40,41 and 43-45 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                     | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

## **DETAILED ACTION**

### ***Response to Amendment***

This Office action has been issued in response to amendment filed 24 April 2007. Claims 1, 4-7, 9, 11-16, 18, 20-24, 27-28, 30, 32-33, 35-36, 38, 40-41, and 43-45 are pending. Applicant's arguments have been carefully and respectfully considered, and some are persuasive, while others are not. Accordingly, objections and rejections have been removed where arguments were persuasive, but rejections have been maintained where arguments were not persuasive. Accordingly, claims 1, 4-7, 9, 11-16, 18, 20-24, 27-28, 30, 32-33, 35-36, 38, 40-41, and 43-45 are rejected, and this action has been made FINAL, as necessitated by amendment.

### ***Claim Objections***

As per claim 14, the phrase "which has be deleted" is incorrect. It should be "which has been deleted".

Claim 27 is objected to for the following informality: in the phrase "in responsive to the request", "responsive" is incorrect. Appropriate correction is required.

As per claim 30, the phrase "wherein the the privacy function" is incorrect. It should be "wherein the ~~the~~ privacy function".

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

Art Unit: 2168

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 4-7, 9, 11-16, 18, 20-24, 27-28, 30, 32-33, 35-36, 38, 40-41, and 43-45 are rejected under 35 U.S.C. 102(b) as being anticipated by Bohrer et al.

As per claims 1, 4-7, 9, 11-16, 18, 20-24, 27-28, 30, 32-33, 35-36, 38, 40-41, and 43-45, Bohrer et al. teach:

1. A method for managing privacy preferences or access to restricted information, comprising (See e.g. [0001], “methods, systems and business methods to enforce privacy preferences on exchanges of personal data across a network”):

tagging restricted or personal information in a content object to distinguish the restricted or personal information from an unrestricted portion of the object content (See e.g. Fig. 2 where, see [0045], “Moreover, a data subject can categorize his/her personal data into multiple View Levels (layers) so that the data in each View Level have the same privacy preference, access and authorization constraints, whereas data in different View Levels have different constraints”);

defining the content object to include the unrestricted portion of the object content in a mark-up language and a link to the restricted or personal information (See e.g. Fig. 2 where, see [0044], “for a specified Authorization Dataset, the specified Privacy Preference Rule is applied for the specified Access List to determine an Authorization Action” and where, see [0029], “this information could be in hypertext markup language”);

parsing the content object to separate privacy preferences or other restriction preferences of an author or owner of the content object from the content object (See e.g. [0049], “FIG. 3 is an expansion of the Privacy Preference Rule 203 in FIG. 2. It explains the data structure for specifying a Privacy Preference Rule for the data requesters in the Access List to access the data

Art Unit: 2168

in the Authorization Dataset”) and to provide access to the privacy preferences or other restriction preferences in response to the content object being collected to satisfy a request (See e.g. Fig. 4a where, see [0078], “A data request identifies a data subject, and includes a request for specific items of data from the data subject” and [0081], “A data response is... the subset of specific data items which were requested and authorized, along with associated privacy declarations representing the data subject’s privacy preferences”); and

distributing the content object based on the privacy preferences or other restriction preferences (See e.g. Fig. 4b where, see [0081], “A data response is... the subset of specific data items which were requested and authorized, along with associated privacy declarations representing the data subject’s privacy preferences”).

2. (Canceled)

3. (Canceled)

4. The method of claim 1, further comprising:

storing the content object (See e.g. [0017], “it allows a data subject to express complex policies on a large set of personal data in a way that is applicable regardless of the specific representation and data model used by enterprises that store that data”); and

providing access to the content object (See e.g. [0017], “it allows a data subject to specify complex privacy preferences that include who can access the data”).

5. The method of claim 1, further comprising:

storing the restricted or personal information in a different location from the content object (See e.g. Fig. 1 where, see [0033], “To facilitate the requests from a Data Subject to setup

Art Unit: 2168

data profiles and privacy policies... The profiles are stored in a Profile Database 123 while the policies are stored in a Policy Database 124"); and

providing access to the restricted or personal information via the link, wherein the link comprises a secure connection (See e.g. Fig. 1 where, see [0032], "Similarly, a Data Requester 105 can use a web browser 106 or some other computer programs 107 to send requests for data 109 as well as receive replies 110 to that request along with any returned data").

6. The method of claim 1, further comprising:

receiving the request for information (See e.g. [0032], "a Data Requester 105 can use a web browser 106 or some other computer programs 107 to send requests for data");

interrogating content sources (See e.g. [0035], "The Profile Responder 116 receives requests for profile information... and uses the Policy authorization engine to check the authorization and privacy policies"); and

collecting any content objects responsive to the request from the content sources (See e.g. [0016], "The data is released only if the privacy declaration of the requester matches the constraints imposed by the data subject via its privacy preferences").

7. The method of claim 6, wherein collecting any content objects responsive to the request comprises using a collection function (See e.g. Fig. 5 where, see [0082], "When the entire request list has been processed, the data to be returned is gathered 516, the response structure is constructed and returned to the requester by the Profile Responder 517").

8. (Canceled)

9. The method of claim 6, further comprising distributing any content object responsive to the request to a privacy function (See e.g. [0030], "This embodiment supports the enforcement

Art Unit: 2168

of privacy preferences in data exchanges according to authorization checks based on the privacy preferences specified by a data subject with the privacy policies of a data requester” where the referenced “authorization checks” are the claimed “privacy functions”).

10. (Canceled)

11. The method of claim 1, further comprising locating or accessing privacy preferences or other restriction preferences using another link (See e.g. Fig. 1 where, see [0032], “Similarly, a Data Requester 105 can use a web browser 106 or some other computer programs 107 to send requests for data 109 as well as receive replies 110 to that request along with any returned data”).

12. The method of claim of claim 9, further comprising comparing the privacy preferences or other restriction preferences of the author or owner of the content object to a content provider’s policies (See e.g. [0003], “In some cases the web site’s privacy policy is compared to the consumer’s policy preferences and warnings are issued when there is a mismatch”).

13. The method of claim 12, further comprising distributing the content object to a requester without any modification to the content object in response to the privacy preferences or other restriction preferences of the author or owner of the content object being consistent with the content provider’s policies (See e.g. [0017], “an independent third party acting as a data-subject’s personal data service and providing various services including... matching privacy policies, gathering data from third parties and releasing and/or authorizing release of data to data requesters”).

14. The method of claim 12, further comprising:

Art Unit: 2168

deleting or replacing the restricted or personal information with default or generic information in response to the privacy preferences or other restriction preferences of the author or owner of the content object being inconsistent with the content provider's policies (See e.g. [0081], "A data response is either a denial, if the request cannot be fulfilled, or the subset of specific data items which were requested and authorized" and Fig. 5 where, see [0082], "If the result is deny, then the data item is not included in the list of data items to be returned in the response 511");

repackaging the content object in response to deleting or replacing the restricted or personal information (See e.g. Fig. 5 where, see [0082], "When the entire request list has been processed, the data to be returned is gathered 516"); and

distributing the repacked content object to a requester without the restricted or personal information which has been deleted or replaced by the default or generic information (See e.g. Fig. 5 where, see [0082], "the response structure is constructed and returned to the requester by the Profile Responder 517").

15. A method for managing privacy or access to restricted information, comprising (See e.g. [0001], "methods, systems and business methods to enforce privacy preferences on exchanges of personal data across a network"):

collecting a content object responsive to a request (See e.g. Fig. 5 where, see [0082], "If authentication succeeds, then the data request is passed to the Policy Authorization Engine which retrieves all Authorization Rules of the data subject specified in the request 503");

accessing privacy preferences or other restriction preferences of an author or owner of the content object (See e.g. Fig. 5 where, see [0082], "the Policy Authorization Engine next



Art Unit: 2168

compares the privacy declarations in the request with the Privacy Preference Rules in the authorization rules for each profile data item name in the request item 506”);

comparing the privacy preferences or other restriction preferences to a content provider’s policies (See e.g. Fig. 5 where, see [0082], “For each data item name in the query and in the request item list, the Policy Authorization Engine retrieves any privacy preferences from the authorization rules. It then performs the Policy-Preference matching process (see FIG. 6) for each data item”);

deleting or replacing private or restricted information with default or generic information in response to the privacy preferences or other restriction preferences being inconsistent with the content provider’s policies (See e.g. Figs. 4a-b where, see [0081], “A data response is either a denial, if the request cannot be fulfilled, or the subset of specific data items which were requested and authorized” and Fig. 5 where, see [0082], “If the result is deny, then the data item is not included in the list of data items to be returned in the response 511”), wherein the content provider collects the content object and has access to the private or restricted information (See e.g. Fig. 7 where, see [0088], “FIG. 7 is a flow diagram of a routine that enables a gather and filtering process carried out to collect data to be returned to a data requester”);

repackaging the content object in response to deleting or replacing the private or restricted information (See e.g. Fig. 5 where, see [0082], “When the entire request list has been processed, the data to be returned is gathered 516”); and

distributing the repacked content object to a requester without the private or restricted information (See e.g. Fig. 5 where, see [0082], “the response structure is constructed and returned to the requester by the Profile Responder 517”).

16. The method of claim 15, further comprising distributing the content object as originally constituted in response to the privacy preferences or other restriction preferences being consistent with the content provider's policies (See e.g. [0033], "To facilitate the requests... for data from Data Requesters, the system must provide several different functionalities, including the ability to... authorize release of data based on authorization rules and privacy policy matching and release data").

17. (Canceled)

18. The method of claim 15, further comprising using a collection function to collect the content object responsive to the request (See e.g. Fig. 5 where, see [0082], "When the entire request list has been processed, the data to be returned is gathered 516, the response structure is constructed and returned to the requester by the Profile Responder 517").

19. (Canceled)

20. The method of claim 15, further comprising distributing any content object in response to the request to a privacy function (See e.g. [0030], "This embodiment supports the enforcement of privacy preferences in data exchanges according to authorization checks based on the privacy preferences specified by a data subject with the privacy policies of a data requester' where the 'authorization checks' are considered 'privacy functions'").

21. The method of claim 20, further comprising parsing the content object to separate the privacy preferences or other restriction preferences from an unrestricted portion of the content object (See e.g. [0049], "FIG. 3 is an expansion of the Privacy Preference Rule 203 in FIG. 2. It explains the data structure for specifying a Privacy Preference Rule for the data requesters in the Access List to access the data in the Authorization Dataset").

22. The method of claim 21, further comprising locating or accessing the privacy preferences or restriction preferences using a link (See e.g. Fig. 1 where, see [0032], “Similarly, a Data Requester 105 can use a web browser 106 or some other computer programs 107 to send requests for data 109 as well as receive replies 110 to that request along with any returned data”).

23. A system for managing privacy preferences or access to restricted information, comprising (See e.g. [0001], “methods, systems and business methods to enforce privacy preferences on exchanges of personal data across a network”):

a server to collect a content object in response to a request (See e.g. Fig. 5 where, see [0082], “If authentication succeeds, then the data request is passed to the Policy Authorization Engine which retrieves all Authorization Rules of the data subject specified in the request 503”);

a privacy function operable on the server to access privacy preferences or other restriction preferences of an author or owner of the content object (See e.g. Fig. 5 where, see [0082], “the Policy Authorization Engine next compares the privacy declarations in the request with the Privacy Preference Rules in the authorization rules for each profile data item name in the request item 506”) and to compare the privacy preferences or other restriction preferences to a content provider’s policies (See e.g. Fig. 5 where, see [0082], “For each data item name in the query and in the request item list, the Policy Authorization Engine retrieves any privacy preferences from the authorization rules. It then performs the Policy-Preference matching process (see FIG. 6) for each data item”), wherein the privacy function deletes or replaces private or restricted information with default or generic information in response to the privacy preferences or restriction preferences being inconsistent with the content provider’s policies (See e.g. Figs. 4a-b where, see [0081], “A data response is either a denial, if the request cannot be

Art Unit: 2168

fulfilled, or the subset of specific data items which were requested and authorized” and Fig. 5 where, see [0082], “If the result is deny, then the data item is not included in the list of data items to be returned in the response 511”), and wherein the privacy function repackages the content object in response to deleting or replacing the private or other restricted information (See e.g. Fig. 5 where, see [0082], “When the entire request list has been processed, the data to be returned is gathered 516”); and

a collection function operable on the server to distribute the repackaged content object to the requester without the private or restricted information (See e.g. Fig. 5 where, see [0082], “the response structure is constructed and returned to the requester by the Profile Responder 517”).

24. The system of claim 23, wherein the privacy function distributes the content object as originally constituted in response to the privacy preferences or other restriction preferences being consistent with the content provider’s policies (See e.g. [0033], “To facilitate the requests... for data from Data Requesters, the system must provide several different functionalities, including the ability to... authorize release of data based on authorization rules and privacy policy matching and release data”).

25. (Canceled)

26. (Canceled)

27. The system of claim 23, wherein the collection function is adapted to interrogate content sources and collect content objects from the content sources in responsive to the request (See e.g. Fig. 1 where, see [0032], “a Data Requester 105 can use a web browser 106 or some other computer programs 107 to send requests for data 109 as well as receive replies 110 to that request along with any returned data”).

28. The system of claim 23, wherein the privacy function comprises a program to access the privacy preferences or other restriction preferences via a link (See e.g. Fig. 1 where, see [0032], “Similarly, a Data Requester 105 can use a web browser 106 or some other computer programs 107 to send requests for data 109 as well as receive replies 110 to that request along with any returned data”).

29. (Canceled)

30. The system of claim 23, wherein the privacy function comprises means for transmitting the content object as originally constituted to the collection function in response to the privacy preferences or restriction preferences being consistent with the content provider’s policies (See e.g. [0033], “To facilitate the requests... for data from Data Requesters, the system must provide several different functionalities, including the ability to... authorize release of data based on authorization rules and privacy policy matching and release data”).

31. (Canceled)

32. A method of making a system for managing privacy preferences or access to restricted information, comprising (See e.g. [0001], “methods, systems and business methods to enforce privacy preferences on exchanges of personal data across a network”):

providing a server to collect a content object in response to a request (See e.g. Fig. 5 where, see [0082], “If authentication succeeds, then the data request is passed to the Policy Authorization Engine which retrieves all Authorization Rules of the data subject specified in the request 503”);

providing a privacy function operable on the server to access privacy preferences or other restriction preferences of an author or owner of the content object (See e.g. Fig. 5 where, see

Art Unit: 2168

[0082], “the Policy Authorization Engine next compares the privacy declarations in the request with the Privacy Preference Rules in the authorization rules for each profile data item name in the request item 506”);

adapting the privacy function to compare the privacy preferences or other restriction preferences to a content provider’s policies (See e.g. Fig. 5 where, see [0082], “For each data item name in the query and in the request item list, the Policy Authorization Engine retrieves any privacy preferences from the authorization rules. It then performs the Policy-Preference matching process (see FIG. 6) for each data item”);

adapting the privacy function to delete or replace private or restricted information with default or generic information in response to the privacy preferences or restriction preferences being inconsistent with the content provider’s policies (See e.g. [0081], “A data response is either a denial, if the request cannot be fulfilled, or the subset of specific data items which were requested and authorized” and Fig. 5 where, see [0082], “If the result is deny, then the data item is not included in the list of data items to be returned in the response 511”);

adapting the privacy function to repackage the content object in response to deleting or replacing the private or other restricted information (See e.g. Fig. 5 where, see [0082], “When the entire request list has been processed, the data to be returned is gathered 516”); and

providing a collection function operable on the server to distribute the repackaged content object to the requester without the private or restricted information (See e.g. Fig. 5 where, see [0082], “the response structure is constructed and returned to the requester by the Profile Responder 517”).

33. The method of claim 32, further comprising adapting the privacy function to distribute the content object as originally constituted in response to the privacy preferences or other restriction preferences being consistent with the content provider's policies (See e.g. [0033], "To facilitate the requests... for data from Data Requesters, the system must provide several different functionalities, including the ability to... authorize release of data based on authorization rules and privacy policy matching and release data").

34. (Canceled)

35. The method of claim 32, further comprising adapting the collection function to interrogate content sources and to collect content objects responsive to the request (See e.g. Fig. 1 where, see [0032], "a Data Requester 105 can use a web browser 106 or some other computer programs 107 to send requests for data 109 as well as receive replies 110 to that request along with any returned data").

36. The method of claim 32, further comprising providing a program in the privacy function to access the privacy preferences or other restricted preferences via a link (See e.g. Fig. 1 where, see [0032], "Similarly, a Data Requester 105 can use a web browser 106 or some other computer programs 107 to send requests for data 109 as well as receive replies 110 to that request along with any returned data").

37. (Canceled)

38. The method of claim 32, further comprising adapting the privacy function to transmit the content object as originally constituted to the collection function in response to the privacy preferences or restriction preferences being consistent with the content provider's policies (See e.g. [0033], "To facilitate the requests... for data from Data Requesters, the system must provide

Art Unit: 2168

several different functionalities, including the ability to... authorize release of data based on authorization rules and privacy policy matching and release data”).

39. (Canceled)

40. A computer-readable medium having computer executable instructions for performing a method, comprising (See e.g. [0001], “methods, systems and business methods to enforce privacy preferences on exchanges of personal data across a network”):

collecting a content object responsive to a request (See e.g. Fig. 5 where, see [0082], “If authentication succeeds, then the data request is passed to the Policy Authorization Engine which retrieves all Authorization Rules of the data subject specified in the request 503”);

accessing privacy preferences or other restriction preferences of an author or owner of the content object (See e.g. Fig. 5 where, see [0082], “the Policy Authorization Engine next compares the privacy declarations in the request with the Privacy Preference Rules in the authorization rules for each profile data item name in the request item 506”);

comparing the privacy preferences or other restriction preferences to a content provider’s policies (See e.g. Fig. 5 where, see [0082], “For each data item name in the query and in the request item list, the Policy Authorization Engine retrieves any privacy preferences from the authorization rules. It then performs the Policy-Preference matching process (see FIG. 6) for each data item”);

deleting or replacing private or restricted information with default or generic information in response to the privacy preferences or restriction preferences being inconsistent with the content provider’s policies (See e.g. [0081], “A data response is either a denial, if the request cannot be fulfilled, or the subset of specific data items which were requested and authorized” and



Art Unit: 2168

Fig. 5 where, see [0082], “If the result is deny, then the data item is not included in the list of data items to be returned in the response 511”), wherein the content provider collects the content object and has access to the private or restricted information (See e.g. Fig. 7 where, see [0088], “FIG. 7 is a flow diagram of a routine that enables a gather and filtering process carried out to collect data to be returned to a data requester”);

repackaging the content object in response to deleting or replacing the private or other restricted information (See e.g. Fig. 5 where, see [0082], “When the entire request list has been processed, the data to be returned is gathered 516”); and

distributing the repacked content object to the requester without the private or restricted information (See e.g. Fig. 5 where, see [0082], “the response structure is constructed and returned to the requester by the Profile Responder 517”).

41. The computer-readable medium having computer executable instructions for performing the method of claim 40, further comprising distributing the content object as originally constituted in response to the privacy preferences or other restriction preferences being consistent with the content provider’s policies (See e.g. [0033], “To facilitate the requests... for data from Data Requesters, the system must provide several different functionalities, including the ability to... authorize release of data based on authorization rules and privacy policy matching and release data”).

42. (Canceled)

43. The computer-readable medium having computer executable instructions for performing the method of claim 40, further comprising distributing any content object responsive to the request to a privacy function (See e.g. [0030], “This embodiment supports the enforcement

Art Unit: 2168

of privacy preferences in data exchanges according to authorization checks based on the privacy preferences specified by a data subject with the privacy policies of a data requester' where the 'authorization checks' are considered 'privacy functions').

44. The computer-readable medium having computer executable instructions for performing the method of claim 43, further comprising parsing the content object to separate the privacy preferences or other restriction preferences from an unrestricted portion of the content object (See e.g. [0049], "FIG. 3 is an expansion of the Privacy Preference Rule 203 in FIG. 2. It explains the data structure for specifying a Privacy Preference Rule for the data requesters in the Access List to access the data in the Authorization Dataset").

45. The computer-readable medium having computer executable instructions for performing the method of claim 44, further comprising locating or accessing the privacy preferences or restriction preferences using a link (See e.g. Fig. 1 where, see [0032], "Similarly, a Data Requester 105 can use a web browser 106 or some other computer programs 107 to send requests for data 109 as well as receive replies 110 to that request along with any returned data").

### ***Response to Arguments***

Applicant's arguments filed 24 April 2007 have been respectfully considered but they are not persuasive.

As per Applicant's argument that Bohrer et al. do not teach "tagging restricted or personal information" in claim 1, the Examiner respectfully disagrees and has cited Fig. 2 where, see [0045], "Moreover, a data subject can categorize his/her personal data into multiple View

Art Unit: 2168

Levels (layers) so that the data in each View Level have the same privacy preference, access and authorization constraints, whereas data in different View Levels have different constraints”.

As per Applicant’s argument that Bohrer et al. do not teach “defining the content object” in claim 1, the Examiner respectfully disagrees and has cited Fig. 2 where, see [0044], “for a specified Authorization Dataset, the specified Privacy Preference Rule is applied for the specified Access List to determine an Authorization Action” and where, see [0029], “this information could be in hypertext markup language”. Further, links are shown broadly in the figures as lines connecting the elements.

As per Applicant’s argument that Bohrer et al. do not teach “parsing the content object” in claim 1, the Examiner respectfully disagrees, and has cited [0049], “FIG. 3 is an expansion of the Privacy Preference Rule 203 in FIG. 2. It explains the data structure for specifying a Privacy Preference Rule for the data requesters in the Access List to access the data in the Authorization Dataset”, Fig. 4a where, see [0078], “A data request identifies a data subject, and includes a request for specific items of data from the data subject” and [0081], “A data response is... the subset of specific data items which were requested and authorized, along with associated privacy declarations representing the data subject’s privacy preferences”.

As per Applicant’s argument that Bohrer et al. do not teach “distributing the content object” in claim 1, the Examiner respectfully disagrees and has cited Fig. 4b where, see [0081], “A data response is... the subset of specific data items which were requested and authorized, along with associated privacy declarations representing the data subject’s privacy preferences”.

As per Applicant’s argument that Bohrer et al. do not teach “deleting or replacing private or restricted information” in claims 15, 23, 32, and 40, the Examiner respectfully disagrees and

Art Unit: 2168

has cited Figs. 4a-b where, see [0081], “A data response is either a denial, if the request cannot be fulfilled, or the subset of specific data items which were requested and authorized”, Fig. 5 where, see [0082], “If the result is deny, then the data item is not included in the list of data items to be returned in the response 511” and Fig. 7 where, see [0088], “FIG. 7 is a flow diagram of a routine that enables a gather and filtering process carried out to collect data to be returned to a data requester”.

As per Applicant’s argument that Bohrer et al. do not teach “repackaging the content object” in claims 15, 23, 32, and 40, the Examiner respectfully disagrees and has cited Fig. 5 where, see [0082], “When the entire request list has been processed, the data to be returned is gathered 516”. As per Applicant’s argument that Bohrer et al. do not teach “distributing the repacked content object” in claims 15, 23, 32, and 40, the Examiner respectfully disagrees and has cited Fig. 5 where, see [0082], “the response structure is constructed and returned to the requester by the Profile Responder 517”. Both steps occur after the private data has been removed from the dataset, see [0081], “A data response is either a denial, if the request cannot be fulfilled, or the subset of specific data items which were requested and authorized”.

### ***Conclusion***

Applicant’s amendment necessitated the new grounds of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Art Unit: 2168

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aaron Sanders whose telephone number is 571-270-1016. The examiner can normally be reached on M-Th 8:00a-5:00p.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tim Vo can be reached on 571-272-3642. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Art Unit: 2168

If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



AJS

802p  
5/29



TIM VO  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100